UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,906	01/17/2001	Ronald P. Doyle	RSW920000096US1	6182

7590 12/08/2004

Jeanine S. Ray-Yarletts
IBM Corporation T81/503
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	6

DATE MAILED: 12/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/761,906	**Applicant(s)** DOYLE ET AL.	
	Examiner Brandon Hoffman	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-120* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22,33-62,73-102 and 113-120* is/are rejected.

7)☒ Claim(s) *1,23-32,41,63-72,81 and 103-112* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *4 and 5*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Double Patenting

1. Claims 1-27, 41-67, 81-107, and 117-120 of this application conflict with claims 1-22 of Application No. 09/764,844 and claims 1-28 of Application No. 09/761,899. 37 CFR 1.78(b) provides that when two or more applications filed by the same applicant contain conflicting claims, elimination of such claims from all but one application may be required in the absence of good and sufficient reason for their retention during pendency in more than one application. Applicant is required to either cancel the conflicting claims from all but one application or maintain a clear line of demarcation between the applications. See MPEP § 822.

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-19, 41-59, and 81-99 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over

claims 1-22 of copending Application No. 09/764,844. Although the conflicting claims are not identical, they are not patentably distinct from each other because the conflicting application is more detailed by specifying a biometric sensor, whereas the instant application refers to a more general portable device. All the limitations of the dependent claims are similar in nature.

4. Claims 1-27, 41-67, and 81-107 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-28 of copending Application No. 09/761,899. Although the conflicting claims are not identical, they are not patentably distinct from each other because the conflicting application is more detailed by specifying a biometric sensor, whereas the instant application refers to a more general portable device. All the limitations of the dependent claims are similar in nature.

5. Claims 37-40, 77-80, and 117-120 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 5, 21, and 22 of copending Application No. 09/764,844. Although the conflicting claims are not identical, they are not patentably distinct from each other because the conflicting application is more detailed by specifying a biometric sensor, whereas the instant application refers to a more general portable device. All the limitations of the dependent claims are similar in nature.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-3, 5-7, 12, 15, 16, 37, 38, 41-43, 45-47, 52, 55, 56, 77, 78, 81-83, 85-87, 92, 95, 96, 117, and 118 are rejected under 35 U.S.C. 102(e) as being anticipated by Bjorn et al. (U.S. Patent No. 6,125,192).

Regarding claims 1, 41, and 81, Bjorn et al. teaches a method/system/computer program product of providing a secure, integrated device with dynamically selectable capabilities, comprising step of:

- Operating a security core which provides security functions (col. 5, line 43 through col. 6, line 27); and
- Securely operably connecting one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device (col. 4, line 39 through col. 5, line 22).

Regarding claims 2, 42, and 82, Bjorn et al. teaches wherein selected ones of the operable connections are made using one or more buses of the secure integrated device (fig. 2, ref. num 205/290).

Regarding claims 3, 43, and 83, Bjorn et al. teaches wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core (col. 4, lines 18-22).

Regarding claims 5, 45, and 85, Bjorn et al. teaches wherein selected ones of the secure operable connections are provided when the security core is manufactured (col. 9, lines 52-62).

Regarding claims 6, 46, and 86, Bjorn et al. teaches wherein the components comprise one or more of (1) input/output components and (2) application processing components (col. 8, lines 4-30).

Regarding claims 7, 47, and 87, Bjorn et al. teaches wherein the step of securely operably connecting further comprises the step of authenticating the operably connected component to the security core (col. 9, line 30 through col. 10, line 7).

Regarding claims 12, 52, and 92, Bjorn et al. teaches further comprising the step of authenticating the security core to the operably connected component (col. 9, line 30 through col. 10, line 7).

Regarding claims 15, 55, and 95, Bjorn et al. teaches wherein the secure integrated device is a pervasive computing device (col. 4, line 65 through col. 5, line 4).

Regarding claims 16, 56, and 96, Bjorn et al. teaches wherein one or more cryptographic keys are securely stored in each component, and wherein at least one of the securely stored keys is used by the step of securely operably connecting each component (col. 5, lines 22-28).

Regarding claims 37, 77, and 117, Bjorn et al. teaches a method/system/computer program product of improving security of transactions in portable devices, comprising steps of:

- Providing security function in a security core of a portable device (col. 5, line 43 through col. 6, line 27);
- Operably connecting one or more components to the security core, wherein each component provides input/output capabilities or application processing capabilities (fig. 2, ref. num 290 and fig. 3 shows 'other system' connected); and
- Verifying authenticity of each operably connected component, such that the security core can vouch for transactions created by the operably connected

components while the operably connected components remain operably connected (col. 4, line 39 through col. 5, line 22).

Regarding claims 38, 78, and 118, Bjorn et al. teaches wherein the verifying authenticity step further comprises the step of performing a security handshake between the security core and the operably connected component upon activation of the step of operably connecting (fig. 7).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 4, 8-11, 13, 14, 17-22, 33-36, 39, 40, 44, 48-51, 53, 54, 57-62, 73-76, 79, 80, 84, 88-91, 93, 94, 97-102, 113-116, 119, and 120 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn et al. (USPN '192) in view of England et al. (U.S. Patent No. 6,330,670).

Regarding claims 4, 39, 44, 79, 84, and 119, Bjorn et al. teaches all the limitations of claims 1, 3 & 37, 38 & 41, 43 & 77, 78 & 81, 83 & 117, 118, respectively, above. However, Bjorn et al. does not teach wherein the performing step uses Secure Sockets Layer encryption to encrypt data or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

England et al. teaches wherein the performing step uses Secure Sockets Layer encryption to encrypt data or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key (see col. 10, lines 4-13 of England et al.).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using SSL for encryption of both endpoints, as taught by England et al., with the method/system/computer program product of Bjorn et al. It would have been obvious for such modifications because SSL uses session keys, this prevents an attacker from disconnecting and reconnecting at a later time after a device has authenticated itself (col. 10, lines 4-13).

Regarding claims 8, 48, and 88, the combination of Bjorn et al. in view of England et al. teaches wherein the step of authenticating provides a unique identifier of the operably connected component to the security core (see col. 9, lines 42-51 of England et al.).

Regarding claims 9, 49, and 89, the combination of Bjorn et al. in view of England et al. teaches wherein the step of securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component (see col. 8, lines 3-37 of England et al.).

Regarding claims 10, 50, and 90, the combination of Bjorn et al. in view of England et al. teaches wherein the step of authenticating is activated during execution of instructions stored on the component, and wherein the execution of the stored instructions is activated by a hardware reset of the component (see col. 8, lines 3-37 of England et al.).

Regarding claims 11, 51, and 91, the combination of Bjorn et al. in view of England et al. teaches wherein instructions for performing the authenticating step are securely stored on the component (see col. 8, lines 18-22 of England et al.).

Regarding claims 13, 53, and 93, the combination of Bjorn et al. in view of England et al. teaches wherein the step of authenticating the operably connected component further comprises using public key cryptography (see col. 8, lines 7-8 of England et al.).

Regarding claims 14, 54, and 94, the combination of Bjorn et al. in view of England et al. teaches wherein the step of authenticating the security core further comprises using public key cryptography (see col. 8, lines 7-8 of England et al.).

Regarding claims 17, 57, and 97, the combination of Bjorn et al. in view of England et al. teaches wherein one or more cryptographic keys are securely stored in the secure integrated device (see fig. 1B, ref. num 164 of England et al.).

Regarding claims 18, 58, and 98, the combination of Bjorn et al. in view of England et al. teaches further comprising the step of authenticating a user of the secure integrated device (see col. 7, lines 45-50 of England et al.).

Regarding claims 19, 59, and 99, the combination of Bjorn et al. in view of England et al. teaches further comprising the step of securely performing a transaction using the secure integrated device (see fig. 3 of England et al.).

Regarding claims 20, 60, and 100, the combination of Bjorn et al. in view of England et al. teaches further comprising the steps of:

- Detecting whether the components remain operably connected to the secure integrated device during the securely performed transaction (fig. 1A); and

- Aborting the securely performed transaction if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction (col. 12, lines 9-12).

Regarding claims 21, 61, and 101, the combination of Bjorn et al. in view of England et al. teaches further comprising steps of:

- Detecting whether all components remain operably connected to the secure integrated device during the securely performed transaction (col. 2, lines 60-67); and
- Marking the securely performed transaction as not secure if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction (col. 11, line 54 through col. 12, line 8).

Regarding claims 22, 62, and 102, official notice is taken that wherein the step of securely performing a transaction further comprises the step of digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device. One of ordinary skill in the art would have been motivated to use digital notarization to support non-repudiation and establish trust between entities.

Regarding claims 33, 73, and 113, the combination of Bjorn et al. in view of England et al. teaches further comprising the steps of dynamically revising functionality in a selected one of the securely operably connected components of the secure integrated device by securely applying a firmware update to the selected one and requiring the selected one to re-authenticate itself to the security core, such that the security core can continue to vouch for the authenticity of the selected one (see col. 12, line 66 through col. 13, line 9 of England et al.).

Regarding claims 34, 74, and 114, the combination of Bjorn et al. in view of England et al. teaches wherein capabilities of the secure integrated device are dynamically revised by subsequent operation of the securely operably connecting step, the subsequent operation being activated upon operably connecting a new component to the security core, wherein the new component authenticates itself to the security core, with a result of the authentication being that the capabilities of the secure integrated device are thereby augmented with capabilities of the new component (see col. 12, line 66 through col. 13, line 9 of England et al.).

Regarding claims 35, 75, and 115, the combination of Bjorn et al. in view of England et al. teaches wherein the security core is located on a selected one of the operably connected components, and wherein the security core and the selected one are connected to a common bus (see fig. 2, ref. num 205/290 of Born et al.).

Regarding claims 36, 76, and 116, the combination of Bjorn et al. in view of England et al. teaches wherein a second security core is located on a selected one of the operably connected components, and wherein the security core and the second security core each provide security functions for one or more components of the secure integrated device (see fig. 3 of Bjorn et al., "other systems" could contain the security core).

Regarding claims 40, 80, and 120, Bjorn et al. teaches all the limitations of claims 37, 38 & 77, 78 & 117, 118, respectively, above. However, Bjorn et al. does not teach wherein each operably connected component has associated therewith a digital certificate, a private cryptographic key and a cryptographically-associated public key, and a unique device identifier that is used to identify data originating from the operably connected component.

England et al. teaches wherein each operably connected component has associated therewith a digital certificate, a private cryptographic key and a cryptographically-associated public key, and a unique device identifier that is used to identify data originating from the operably connected component (col. 12, lines 53-65).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine each operably connected component has associated therewith a digital certificate, a private cryptographic key and a cryptographically-associated public key, and a unique device identifier that is used to identify data originating from the operably connected component, as taught by England et al., with the method/system/computer program product of Bjorn et al. It would have been obvious for such modifications because the digital certificates, keys, and unique identifiers serve to identify both the security core and the connected components (see col. 12, lines 53-65 of England et al.).

Allowable Subject Matter

10. Claims 23-32, 63-72, and 103-112 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Objections

11. Claims 1, 41, and 81 are objected to because of the following informalities: claims recite "...securely operably connecting...". Applicant is advised to revise the grammar. Appropriate correction is required.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Okada (U.S. Patent No. 6,704,872).

b. Howard et al. (U.S. Patent No. 6,442,690).

c. Murphy, Jr. et al. (U.S. Patent No. 6,070,245).

d. Bakhle et al. (U.S. Patent No. 6,021,201).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoff
BH

AU2131
12/1/04